REMARKS

Reconsideration of this application is respectfully requested.

In response to the rejection of claims 1-11 under 35 U.S.C. § 112, second paragraph, the claims have been amended above so as to avoid the adjective "unique" in connection with the description of "random numbers". Instead, the claims are now more particularly describe the members of the claimed list to comprise non-duplicated random numbers. It is believed to be clear that the claimed list comprises non-duplicated members so that a different one of those members can be selected as the included data with each transmitted data packet, the recipient server then being able to check such included data by comparing it to its own list of the same non-duplicated members. Only if the recipient server finds that the included data to also exist in its own list does it accept and acknowledge receipt back to the sending server. Preferably, the acknowledgement message includes data identifying the position of the included data within the list that is commonly shared between the sending and receiving server. In this way, the acknowledgement message may itself be checked by the sending server to insure that it was properly received by an authentic authorized recipient server (e.g. by detecting whether the acknowledgement message properly identifies the position of the selected and included member of the list for that particular packet).

Accordingly, it is not believed that there can be any undue ambiguity in the intended meaning of recitations throughout claims 1-11 which are variously directed to these features.

The rejection of claims 1-11 under 35 U.S.C. § 103 as allegedly being made "obvious" based on Perlman '865 in view of Thomas '899 is respectfully traversed.

As explained in applicants' submission of October 26, 2005, Perlman is essentially irrelevant with respect to the applicants' claimed invention. It is merely an example of admitted

prior art already described in the background section of the applicants' specification. In particular, Perlman uses public key cryptography processes which require encryption/decryption processing for each data packet.

The applicants' invention is directed toward an alternate approach which may be somewhat less secure, but which is still highly secure and which avoids the extensive overhead required for encryption/decryption processes associated with every exchange of a data packet as in prior art such as Perlman.

The Examiner incorrectly alleges that Perlman even meets the recitations of sections (i), (ii) and (iv) in claim 1. For example, Perlman does <u>not</u> store a list of non-duplicated random numbers and a first server and send a copy of that list to authorized recipient servers by secure communication means. The Examiner alleges that such is taught by Perlman in several locations—but that is not the case:

> <u>Abstract</u>
>
> There is no mention of any "list" in the Abstract. If the Examiner is referring to the computed entire routing path as comprising a sequence of nodes in the communication network that is computed and enclosed within the packet being sent, this is of course not a list of non-duplicated random numbers and it is not sent by secure means to recipient to authorize recipient servers <u>prior</u> to the sending of a data packet. Instead, it is merely <u>part of</u> the data packet which is transmitted using encryption/decryption overhead—for every packet transmitted. This is, of course, exactly contrary to the applicants' teachings.
>
> <u>Column 3, lines 5-6</u>
>
> This passage merely explains that each data packet is assigned a sequence number by the originating node which is incremented for each successive originated message from that node. Of course, sequence numbers are perhaps also useful but sequentially assigned sequence numbers also fall far short of the applicants' claimed stored list of non-duplicated random numbers. Furthermore, there is no indication that an entire listing of sequence numbers is ever accumulated into a defined "list" nor that any such accumulated composite "list" is ever securely communicated to authorized recipient servers, etc.

<u>Column 4, lines 54-60</u>

This passage merely explains that devices served by the nodes in the network can communicate with each other by sending data packets over the network. This is an unsurprising statement but it has nothing to do with the claimed novel features of applicants' invention.

<u>Column 5, lines 33-40, 51-55, 58-59 and 65-67</u>

This passage simply explains that each node in the network is assigned a unique identification number and a unique pair of associated encryption keys (one private, the other public). It goes on to describe a process whereby the public keys for the various nodes are exchanged between the nodes. However, a listing of public keys to be used thereafter in decryption processes is <u>not</u> any teaching or suggestion of applicants' invention wherein one of the non-duplicated random numbers in a stored list is selected and included in a transmitted data packet, the selected random number not having previously been selected for inclusion in a data packet to be transmitted. Indeed, once the public keys are exchanged between the nodes, there is no need for any further transmission of the public keys this really is a graphic illustration of the stark <u>difference</u> between the Perlman teaching which requires the use of encryption/decryption overhead with each data packet exchange at both the transmitting and sending servers.

<u>Column 7, lines 44-46</u>

This passage of text merely describes the sending of a packet after it has been encrypted and describes transmission queues in the manner in which a PACKET SEND flag is utilized in processing such a queue for transmission. It has essentially nothing to do with anything in the applicants' claims.

With such a glaring fundamental deficiency in Perlman '865 vis-à-vis independent claims 1, 4, 6 and 10, it is not believed necessary to discuss the further deficiencies of this reference with respect to the remainder of these independent claims nor with respect to the added features of the dependent claims.

The Examiner recognizes that Perlman does not teach random numbers or selecting a random number from a list for inclusion in a data packet, the selected random number not having previously been selected and included in a prior data packet, etc. For this admitted deficiency, the Examiner relies upon Thomas '899. However, Thomas does not supply such admitted deficiencies (nor the further deficiencies noted above with respect to Perlman). The Examiner

alleges that Thomas does teach a unique random number at Column 4, lines 63-67, Column 5, lines 12-20 and claim 1, steps a) and b). This assertion is respectfully traversed.

The first cited passage merely notes the difficulty of keeping track of sequence numbers and a very large number space. There is no indication that the sequence numbers are randomly selected or randomly generated or otherwise having anything to do with randomness. The second cited passage simply recognizes the burden of keeping track of sequence numbers efficiently in a very large sequence number space. Claim 1 at steps a) and b) merely recite assigning sequence numbers <u>in order</u> to a series of transmitted packets and defining an acceptable <u>range</u> of such sequence numbers at the destination. Again, there is nothing in this having anything to do with randomness. Indeed, the whole thrust of Thomas is an attempt to keep track of sequence numbers in a very large number space by defining only a relatively smaller sub-space within a defined window of acceptable values for use over a given period of time. If anything, the Thomas teaching is the antithesis of randomness.

In view of the fundamental deficiencies already discussed with respect to both cited references, it is not believed necessary at this time to detail the still further deficiencies of both these references with respect to the remainder of the independent claims or the additional limitations added by the dependent claims.

The Examiner's attention is also directed to new claims 12-18. It will be seen that independent claim 12 is directed to a method for reducing the possibility that an unauthorized data packet is conveyed over a network of interconnected servers in a packet data communication network. The method requires generating a list of unique data values and storing that list of first server, securely sending a copy of that list to at least one other server authorized to communicate data packets with the first server and also locally storing such received copy at such at least one other authorized recipient server. Claim 12 also requires including at least one

selected not previously used member of the stored list of data values in an authorized data packet being sent from a sending server to a receiving server and accepting the received data packet at a receiving server only if the included data value is present in the locally stored list and has not been previously used. Dependent claims 13-18 add yet further patentable distinction to the claimed invention.

Accordingly, this entire application is now believed to be in allowable condition and a formal notice to that effect is respectfully solicited.

Respectfully submitted,

NIXON & VANDERHYE P.C.

By: Larry S. Nixon
Larry S. Nixon
Reg. No. 25,640

LSN:dm
901 North Glebe Road, 11th Floor
Arlington, VA 22203-1808
Telephone: (703) 816-4000
Facsimile: (703) 816-4100